The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
12/02/2020

SUBJECT:
A Vulnerability in Mozilla Thunderbird Could Allow for Arbitrary Code Execution

OVERVIEW:
A vulnerability has been discovered in Mozilla Thunderbird, which could allow for arbitrary code execution. Mozilla Thunderbird is an email client. Successful exploitation of this vulnerability could allow for arbitrary code execution. Depending on the privileges associated with the user an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
There are no reports of this vulnerability being exploited in the wild.

SYSTEMS AFFECTED:

- Mozilla Thunderbird versions prior to 78.5.1

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
A vulnerability has been discovered in Mozilla Thunderbird, which could allow for arbitrary code execution. This vulnerability exists due incorrect parsing of SMTP server response codes. Depending on processor architecture and stack layout, this leads to stack corruption that may be exploitable. Successful exploitation of this vulnerability could allow for arbitrary code execution. Depending on the privileges associated with the user an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users

whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate updates provided by Mozilla to vulnerable systems, immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:

Mozilla:

https://www.mozilla.org/en-US/security/advisories/mfsa2020-53/

CVE:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26970